REMARKS

The foregoing amendments are responsive to the October 12, 2006 Office Action. Applicant respectfully request reconsideration of the present application in view of the foregoing amendments and the following remarks.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Response to Rejection of Claims 13 and 15-16 Under 35 U.S.C. 103(a)

The Examiner rejected Claims 13 and 15-16 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,351,811 to Groshon et al. ("Groshon"), in view of European Patent No. 467,239 to Bianco, and further in view of U.S. Patent No. 5,537,585 to Blickenstaff et al. (Blickenstaff), U.S. Patent No. 6,880,083 to Korn, and U.S. Patent No. 5,812,398 to Nielsen.

Nielsen teaches a firewall circumvention method wherein a file to be backed up on the escrow computer is embedded in an email message sent from the host computer to the escrow computer. Thus, Nielsen teaches a method for circumventing a firewall to send encrypted data from the public side of the firewall to the protected side of the firewall. Nielsen does not teach or suggest sending a request from the public side of the firewall and then sending data from the private side of the firewall to a server on the public side of the firewall.

By contrast, Applicant claims a system wherein the firewall is not circumvented. Rather the data is stored unencrypted behind the firewall. When replacement data is needed for the public server, the data is encrypted and sent through the firewall. Thus, the combination of Nielsen with Groshon, Bianco, Blickenstaff and Korn does not yield or suggest the claimed invention.

Regarding Claim 13, the cited prior art does not teach or suggest an anti-alteration system for web-content having a public-web-server configured to create safe-web-files encrypted from original web-content including one or more types of static files and one or more types of dynamic files, and configured to provide HTTP web server functions, a private-web-server configured to provide the original web-content the public-web-server provided to the private-web-server through a firewall, wherein when a web visitor's request is received, the public-web-server is configured to verify that the safe-web-file has not been improperly altered, deleted or replaced,

the public-web-server further configured to decrypt one or more of the safe-web-files and respond to the visitor, and the public-web-server further configured to automatically send a recovery request to the private-web-server when the public-web-server detects an unauthorized alteration of the safe-web-files, the private-web-server, in response to the recovery request, configured to send the safe-web-files to the public server.

Regarding Claim 15, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 13, further comprising a real-time-check module used on the public-web-server computer for linking to a decryption module, wherein the decryption module is configured to decrypt one or more of the safe-web-files in response to an HTTP request received from the web visitor.

Regarding Claim 16, the cited prior art does not teach or suggest the anti-alteration system as recited in Claim 15, further comprising a real-time-check module configured to use symmetric-key encryption to decrypt one or more of the safe-web-files when the web visitor's request is received.

Accordingly, Applicant asserts that Claims 13 and 15-16 are allowable over the prior art, and Applicant requests allowance of Claim 13 and 15-16.

Response to Rejection of Claim 14 Under 35 U.S.C. 103(a)

The Examiner rejected Claim 14 under 35 U.S.C. 103(a) as being unpatentable over the modified Groshon, Korn, Bianco, Blickenstaff, and Neilson.

As discussed above, Applicant respectfully submits that the cited combination of prior art references and modifications to the teachings of the references are non-obvious.

Regarding Claim 14, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 13, wherein the encryption comprises chaos encryption technology to do encryption and decryption of the web-content for increasing the web server response speed and increasing security strong of whole system.

Response to Rejection of Claims 17-28 Under 35 U.S.C. 103(a)

The Examiner rejected Claims 17-28 under 35 U.S.C. 103(a) as being unpatentable over the modified Groshon, Bianco, Neilson and Blickenstaff, in view of Menezes et al. (Handbook of Applied Cryptography) and further in view of Thomson.

As discussed above, Applicant respectfully submits that the cited combination of prior art references and modifications to the teachings of the references are non-obvious.

Regarding Claim 17, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 16, wherein the symmetric-key encryption is selected from a group consisting essentially of DES, 3DES and AES.

Regarding Claim 18, the cited prior art does not teach or suggest an anti-alteration system for web-content having a public-web-server configured to store safe-web-contents that have been provided with header information including a MAC (Message Authentication Code) generated from the original web-content, and properties of the original-web-content including, name, size, date, and location thereof, a private-web-server configured to store the original web-content the public-web-server provided to the private-web-server through a firewall, the private-web-server configured to separate the header information from a requested safe-web-file, and using the MAC (Message Authentication Code) included in the header information to check an authenticity of the safe-web-file, and the public-web-server configured to add new header information to the original web-content to create a new safe-web-file on the private-web-server computer when an unauthorized alteration of the safe-web-file is detected, wherein the new safe-web-file is sent to the public-web-server computer to automatically restore the altered safe-web-file.

Regarding Claim 19, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 18, further comprising a real-time-check module used on the public-web-server computer for linking to an authentication module, wherein the authentication module is configured to provide authentication of the safe-web-file in response to a request received from the web visitor though http protocol.

Regarding Claim 20, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 19, wherein the real-time-check module uses a message authentication technology using chaos theory to check whether the safe-web-content has been altered.

Regarding Claim 21, the cited prior art does not teach or suggest he anti-alteration system, as recited in Claim 18, wherein the real-time-check module that is configured to link the public-web-server services by using at least one message authentication technology selected from a group consisting essentially of MD4, MD5, and SHA.

Regarding Claim 22, the cited prior art does not teach or suggest an anti-alteration system for web-content having a public-web-server computer, configured to store safe-web-files which have been encrypted from original web-contents and have been provided with header information, the header information including a MAC (Message Authentication Code) generated from authentication checking the original web-content and properties including name, size, date, and storage location thereof, a private-web-server computer which retains the original web-content and which is provided to the public-web-server computer through a firewall, a real-time-check module, in response to a web visitor's request safe-web file, the real-time-check module configured to separate the a header information from the safe-web-file using a MAC (Message Authentication Code) included in the header information to authenticate the safe-web-file by comparing the header information with separate header information, and a recovery module, when an unauthorized alteration of the safe-web-file is detected, the recovery module configured to encrypt the original web-content and add header information to the original web-content to create a new safe-web-file on the private-web-server computer, sending the new safe-web-file to the public-web-server computer to automatically restore the safe-web-file which has been altered.

Regarding Claim 23, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 22, wherein the recovery module uses chaos encryption technology to do encryption and decryption.

Regarding Claim 24, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 22, wherein the real-time-check module is configured to provide authentication of the safe-web-file in response to a request received from the web visitor though http protocol.

Regarding Claim 25, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 23, wherein the real-time-check is configured to use a symmetric-key encryption to decrypt the safe-web-contents in response to the web visitor's request.

Regarding Claim 26, the cited prior art does not teach or suggest the anti-alteration system, recited in Claim 25, wherein the symmetric-key encryption is selected from a group consisting essentially of DES, 3DES, RC4 and AES.

Regarding Claim 27, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 24, wherein the real-time-check module uses a message authentication technology using chaos theory to check whether the safe-web-content has been altered.

Regarding Claim 28, the cited prior art does not teach or suggest the anti-alteration system, as recited in Claim 24, wherein the real-time-check module uses at least one of MD4, MD5, and SHA for message authentication.

Accordingly, Applicant asserts that Claims 17-28 are allowable over the prior art, and Applicant requests allowance of Claim 17-28.

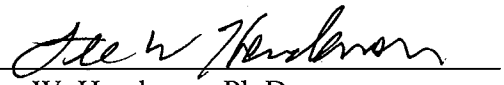
Summary

Applicant respectfully assert that Claims 13-28 are in condition for allowance, and Applicant request allowance of Claims 13-28. If there are any remaining issues that can be resolved by a telephone conference, the Examiner is invited to call the undersigned attorney at (949) 721-6305 or at the number listed below.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: March 22, 2007

By: 

Lee W. Henderson Ph.D.
Registration No. 41,830
Attorney of Record
Customer No. 20,995
(949) 760-0404

3170254//ld
120106